



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,996	12/10/2001	Stephen Carter	010079	3525

23696 7590 02/08/2005

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER

FOX, BRYAN J

ART UNIT	PAPER NUMBER
----------	--------------

2686

DATE MAILED: 02/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/015,996

Applicant(s)

CARTER, STEPHEN

Examiner

Bryan J Fox

Art Unit

2686

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 October 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

Claim 4 is objected to because of the following informalities: "the send/talk key" should be changed to "a send/talk key". There is insufficient antecedent basis to refer to it as, "the send/talk key." Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 11 and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Tanaka et al (US005493693A).

Regarding claim 11, Tanaka et al discloses a secure mobile communication system where if the engaged communication channel were shifted from the digital mode to the analog mode, then the mobile radio station PS generates an alarm to warn the user of the change of the actually engaged communication channel so that the user can easily be aware of this shift, then he can change the subject or terminate the communication (see column 11, lines 21-35), which reads on the claimed "in a wireless handset capable of operating in clear and secure modes, a method of transitioning from secure mode to clear mode during a call." Also, a mode-shift rejecting switch may be provided allowing a user to reject a shift into analog mode (see column 11, lines 21-48), which reads on the claimed "sending at least one message to request going to a clear

mode; confirming transition to the clear mode as received in response to the message; and receiving at least one message authorizing a clear call request," wherein the message from the mobile discontinuing the handoff or allowing the handoff reads on the message authorizing a clear call request.

Regarding claim 21, Tanaka et al discloses a secure mobile communication system where if the engaged communication channel were shifted from the digital mode to the analog mode, then the mobile radio station PS generates an alarm to warn the user of the change of the actually engaged communication channel so that the user can easily be aware of this shift, then he can change the subject or terminate the communication (see column 11, lines 21-35), which reads on the claimed "in a wireless handset capable of operating in clear and secure modes, a method of transitioning from secure mode to clear mode during a call." Also, a mode-shift rejecting switch may be provided allowing a user to reject a shift into analog mode (see column 11, lines 21-48), which reads on the claimed "means for sending at least one message to request going to a clear mode; means for confirming transition to the clear mode as received in response to the message; and means for receiving at least one message authorizing a clear call request," wherein the message from the mobile discontinuing the handoff or allowing the handoff reads on the message authorizing a clear call request.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-3, 5, 12-15 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walter et al (US006151677A) in view of Mannisto (US005805084A).

Regarding claim 1, Walter et al discloses a wireless telephone system for security where a keypad 152 includes a switch or other means, such as a pushbutton, for allowing the user to activate a secure transmission mode (see column 5, lines 34-37). Walter et al fails to expressly disclose that the pushbutton must be pressed for a certain amount of time.

In a similar field of endeavor, Mannisto discloses a system where in order to set a keyboard lock, a user depresses and holds the key for a given delay period. If the button is not pressed for a certain amount of time, the phone does not enter the keyboard lock state (see column 2, line 62 – column 3, line 3). Further, if the phone is in the auto-locked state, only the unlock sequence will register in the phone once it is locked (see column 3, lines 35-45), satisfying the condition of “unless the handset is currently in either secure-only mode or auto secure mode.”

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Walter et al with Mannisto so that the holding of the key sets the secure mode in order to avoid the need for a separate key which takes up space in the keypad and increases manufacturing costs as suggested by Mannisto (see column 1, lines 60-61).

Regarding claim 2, the combination of Walter et al and Mannisto discloses a system where a PIN is used to unlock the security features (see Walter et al column 4, lines 50-52 and column 7, lines 6-10 and figure 3).

Regarding claim 3, the combination of Walter et al fails to disclose the predetermined amount of time is about two seconds.

In a similar field of endeavor, Mannisto discloses a system where a suitable delay for the key to be pressed and held down for is roughly 0.5-2 seconds (see Mannisto column 3, line 3).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Walter et al with Mannisto so that the holding of the key sets the secure mode in order to avoid the need for a separate key which takes up space in the keypad and increases manufacturing costs as suggested by Mannisto (see column 1, lines 60-61).

Regarding claim 5, the combination of Walter et al and Mannisto discloses that after the phone is powered on, the user unlocks it by entering a PIN (see Walter et al column 7, lines 6-10 and figure 3), which reads on the claimed "the step of entering a PIN number is entered each time the handset is activated".

Regarding claim 12, Walter et al discloses a wireless telephone system for security where a keypad 152, which reads on the claimed "user-interface capable of being depressed", includes a switch or other means, such as a pushbutton, for allowing the user to activate a secure transmission mode (see column 5, lines 34-37). Walter et al fails to expressly disclose that the pushbutton must be pressed for a certain amount of time.

Mannisto discloses a system where in order to set a keyboard lock, a user depresses and holds the key for a given delay period. If the button is not pressed for a certain amount of time, the phone does not enter the keyboard lock state (see column 2, line 62 – column 3, line 3). This system must include the circuit for detecting the amount of time a key is depressed for as claimed. Further, if the phone is in the auto-locked state, only the unlock sequence will register in the phone once it is locked (see column 3, lines 35-45), satisfying the condition of "unless the handset is currently in either secure-only mode or auto secure mode."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Walter et al with Mannisto so that the holding of the key sets the secure mode in order to avoid the need for a separate key which takes up space in the keypad and increases manufacturing costs as suggested by Mannisto (see column 1, lines 60-61).

Regarding claim 13, Walter et al discloses a wireless telephone system for security where a keypad 152 includes a switch or other means, such as a pushbutton, for allowing the user to activate a secure transmission mode (see column 5, lines 34-

Art Unit: 2686

37). Walter et al fails to expressly disclose that the pushbutton must be pressed for a certain amount of time.

Mannisto discloses a system where in order to set a keyboard lock, a user depresses and holds the key for a given delay period. If the button is not pressed for a certain amount of time, the phone does not enter the keyboard lock state (see column 2, line 62 – column 3, line 3). Further, if the phone is in the auto-locked state, only the unlock sequence will register in the phone once it is locked (see column 3, lines 35-45), satisfying the condition of “unless the handset is currently in either secure-only mode or auto secure mode.”

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Walter et al with Mannisto so that the holding of the key sets the secure mode in order to avoid the need for a separate key which takes up space in the keypad and increases manufacturing costs as suggested by Mannisto (see column 1, lines 60-61).

Regarding claim 14, the combination of Walter et al and Mannisto discloses a system where a PIN is used to unlock the security features (see Walter et al column 4, lines 50-52 and column 7, lines 6-10 and figure 3), which reads on the claimed “means for entering a personal identification number (PIN) to register as a secure user”.

Regarding claim 15, Walter et al fails to expressly disclose the predetermined amount of time is about 2 seconds.

In a similar field of endeavor, Mannisto discloses a system where a suitable delay for the key to be pressed and held down for is roughly 0.5-2 seconds (see Mannisto column 3, line 3).

Regarding claim 17, the combination of Walter et al and Mannisto discloses that after the phone is powered on, the user unlocks it by entering a PIN (see Walter et al column 7, lines 6-10 and figure 3), which reads on the claimed "the step of entering a PIN number is entered each time the handset is activated".

Claims 4 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walter et al in view of Mannisto as applied to claim 1 above, and further in view of Alanara et al (US005845205A).

Regarding claims 4 and 16, the combination of Walter et al and Mannisto fails to expressly disclose that the key pressed down is the send/talk key.

In a similar field of endeavor, Alanara et al discloses a phone system where a function is assigned to holding down the "send" key (see column 3, lines 50-61).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the combination of Walter et al and Mannisto so that the send key is held down in order to provide a more intuitive interface.

Claims 6, 7, 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walter et al and Mannisto as applied to claim 2 above, and further in view of Harris et al (US006442406B1).

Regarding claims 6 and 18, the combination of Walter et al and Mannisto fails to expressly disclose the disabling of the telephone if the PIN is incorrectly entered a number of times.

Harris et al discloses a system requiring entry of a code to change operating parameters (see column 1, lines 60-67), but when the code entry is not correct a conventional lockout routine is executed (see column 1, line 67 – column 2, line 6), which reads on the claimed “disabling the handset if the PIN number is incorrectly entered more than a predetermined number of times”.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the combination of Walter et al and Mannisto to include the above disabling of the telephone if the PIN is entered incorrectly a number of times in order to enhance the security of the device by making it more difficult for an unauthorized user to break the code.

Regarding claim 7, the combination of Walter et al, Mannisto and Harris et al discloses between 3 and 5 tries as an exemplary number of incorrect entries (see Harris et al column 2, lines 2-6). The combination of Walter et al, Mannisto and Harris et al fails to expressly disclose 7 as the number of tries for entering a PIN however this difference is not critical to the invention and would not render the claimed invention patentable over the disclosed invention because both provide the end result of preventing an unauthorized user from the functions the PIN is protecting. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the combination of Walter et al, Mannisto and Harris et al such that

Art Unit: 2686

the phone is disabled after 7 incorrect PIN entries in order to further prevent an unauthorized user from gaining access to the functions the PIN is protecting.

Regarding claim 8, the combination of Walter et al, Mannisto fails to expressly disclose that the predetermined number of times is 3.

In a similar field of endeavor, Harris et al discloses between 3 and 5 tries as an exemplary number of incorrect entries (see Harris et al column 2, lines 2-6).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the combination of Walter et al and Mannisto to include the above disabling of the telephone if the PIN is entered incorrectly a number of times in order to enhance the security of the device by making it more difficult for an unauthorized user to break the code.

Claims 9, 10, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chapman, Jr et al (US006704567B1) in view of Walter et al.

Regarding claim 9, Chapman, Jr et al discloses a wireless communications device that includes the ability of the wireless handset user to press a "private" key either during or before engaging in a call, which sends a "private" message via the command channel to the wireless network node device (see column 11, lines 36-43), which reads on the claimed "sending at least one message to request making a secure call". The network node checks its resources and the priorities of the current request versus the resources being used (see column 11, lines 53-60) and responds (see step 1304, figure 13), which reads on the claimed "receiving at least one message

Art Unit: 2686

authorizing a secure call request". Chapman, Jr et al fails to disclose entering a PIN as requested in response to the request to make a secure call.

In a similar field of endeavor, Walter et al discloses a system where a PIN is used to unlock the security features (see Walter et al column 4, lines 50-52 and column 7, lines 6-10 and figure 3).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Chapman, Jr et al with Walter et al to include the above PIN authorization in order to prevent unauthorized users from entering the secure mode.

Regarding claim 10, Chapman, Jr et al discloses a wireless communications device that includes the ability of the wireless handset user to press a "private" key either during or before engaging in a call, which sends a "private" message via the command channel to the wireless network node device (see column 11, lines 36-43), which reads on the claimed "sending at least one message to request going into secure mode". The network node checks its resources and the priorities of the current request versus the resources being used (see column 11, lines 53-60) and responds (see step 1304, figure 13), which reads on the claimed "receiving at least one message authorizing a secure call request". Chapman, Jr et al fails to disclose entering a PIN as requested in response to the request to make a secure call.

In a similar field of endeavor, Walter et al discloses a system where a PIN is used to unlock the security features (see Walter et al column 4, lines 50-52 and column 7, lines 6-10 and figure 3).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Chapman, Jr et al with Walter et al to include the above PIN authorization in order to prevent unauthorized users from entering the secure mode.

Regarding claim 19, Chapman, Jr et al discloses a wireless communications device that includes the ability of the wireless handset user to press a "private" key either during or before engaging in a call, which sends a "private" message via the command channel to the wireless network node device (see column 11, lines 36-43), which reads on the claimed "means for sending at least one message to request making a secure call". The network node checks its resources and the priorities of the current request versus the resources being used (see column 11, lines 53-60) and responds (see step 1304, figure 13), which reads on the claimed "means for receiving at least one message authorizing a secure call request". Chapman, Jr et al fails to disclose entering a PIN as requested in response to the request to make a secure call.

In a similar field of endeavor, Walter et al discloses a system where a PIN is used to unlock the security features (see Walter et al column 4, lines 50-52 and column 7, lines 6-10 and figure 3).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Chapman, Jr et al with Walter et al to include the above PIN authorization in order to prevent unauthorized users from entering the secure mode.

Regarding claim 20, Chapman, Jr et al discloses a wireless communications device that includes the ability of the wireless handset user to press a "private" key either during or before engaging in a call, which sends a "private" message via the

command channel to the wireless network node device (see column 11, lines 36-43), which reads on the claimed "means for sending at least one message to request going into secure mode". The network node checks its resources and the priorities of the current request versus the resources being used (see column 11, lines 53-60) and responds (see step 1304, figure 13), which reads on the claimed "means for receiving at least one message authorizing a secure call request". Chapman, Jr et al fails to disclose entering a PIN as requested in response to the request to make a secure call.

In a similar field of endeavor, Walter et al discloses a system where a PIN is used to unlock the security features (see Walter et al column 4, lines 50-52 and column 7, lines 6-10 and figure 3).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Chapman, Jr et al with Walter et al to include the above PIN authorization in order to prevent unauthorized users from entering the secure mode.

Claims 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tanaka et al in view of Mannisto et al.

Regarding claim 22, Tanaka et al discloses a secure mobile communication system where a user of the mobile radio station can operate a mode assigning switching 34 in order to designate either the digital mode or the analog mode whichever the one desired by the user himself (see column 5, lines 11-25), which reads on the claimed "entering a secure mode if the handset is currently in a clear mode." If the engaged communication channel were shifted from the digital mode to the analog

Art Unit: 2686

mode, then the mobile radio station PS generates an alarm to warn the user of the change of the actually engaged communication channel so that the user can easily be aware of this shift, then he can change the subject or terminate the communication (see column 11, lines 21-35). Also, a mode-shift rejecting switch may be provided allowing a user to reject a shift into analog mode (see column 11, lines 21-48), which reads on the claimed "entering a clear mode if the handset is currently in a secure mode and a user confirms the transition from the secure mode to the clear mode," and, "staying in a secure mode if the handset is currently in a secure mode and a user does not confirm the transition from the secure mode to the clear mode." Tanaka et al fails to expressly disclose that the switch must be pressed for a predetermined amount of time.

In a similar field of endeavor, Mannisto discloses a system where in order to set a keyboard lock, a user depresses and holds the key for a given delay period (see column 2, line 62 – column 3, line 3), which reads on the claimed "pressing a key for a time period greater than the predetermined amount of time." If the button is not pressed for a certain amount of time, the phone does not enter the keyboard lock state (see column 2, line 62 – column 3, line 3), which reads on the claimed "if the key is held for a time period less than the predetermined amount of time, staying in a current mode."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Tanaka et al with Mannisto so that the holding of the key sets the secure mode in order to avoid the need for a separate key which takes up space in the keypad and increases manufacturing costs as suggested by Mannisto (see column 1, lines 60-61).

Regarding claim 23, the combination of Tanaka et al and Mannisto discloses a mode-shift rejecting switch may be provided allowing a user to reject a shift into analog mode (see Tanaka et al column 11, lines 21-48), which reads on the claimed "a secure-only mode without fall back to the clear mode if the handset is currently in a secure-only mode."

Regarding claim 24, the combination of Tanaka et al and Mannisto discloses that under normal operation, if a digital channel is not available, an analog channel may be used (see column 11, lines 21-35), which reads on the claimed "entering a secure mode includes entering the secure mode with fall back to the clear mode."

Regarding claim 25, the combination of Tanaka et al and Mannisto discloses that under normal operation, if a digital channel is not available, an analog channel may be used (see column 11, lines 21-35), which reads on the claimed "entering a secure mode includes entering the secure mode with fall back to the clear mode."

Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tanaka et al in view of Mannisto as applied to claim 22 above, and further in view of Walter et al.

Regarding claim 26, the combination of Tanaka et al and Mannisto fails to expressly disclose the requiring of a PIN from a user.

In a similar field of endeavor, Walter et al discloses a system where a PIN is used to unlock the security features (see Walter et al column 4, lines 50-52 and column 7, lines 6-10 and figure 3).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Tanaka et al and Mannisto with Walter et al to include the above PIN authorization in order to prevent unauthorized users from entering the secure mode.

Response to Arguments

Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Art Unit: 2686

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bryan J Fox whose telephone number is (703) 305-8994. The examiner can normally be reached on Monday through Friday 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Marsha Banks-Harold can be reached on (703) 305-4379. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BJF


CHARLES APPIAH
PRIMARY EXAMINER